UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SANDRA M. RINEER,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	**Civil Action No. 07-3739**
	)	
EXPERIAN INFORMATION SOLUTIONS, INC.,	)	
	)	
	)	
Defendant.	)	

DEFENDANT EXPERIAN INFORMATION SOLUTIONS, INC.'S MOTION FOR ENTRY OF PROTECTIVE ORDER

INTRODUCTION

Defendant Experian Information Solutions, Inc. ("Experian") uses a unique and highly sophisticated computer system to collect, manage, and safeguard credit information on more than 200 million consumers. Over several decades, Experian has invested tens of millions of dollars and countless hours of employee time developing its system to achieve maximum possible accuracy of consumer credit information. The system embodies a wealth of accumulated knowledge and experience, and is the "Crown Jewel" of Experian's business. Indeed, it *is* Experian's business.

Plaintiff seeks the disclosure of some of the most highly confidential, proprietary documents relating to Experian's system, including manuals of system codes and reports revealing the system's structure and architecture. Experian has agreed to produce relevant portions of almost all of those documents, but needs the protection of the Proposed Protective Order. *See* Proposed Protective Order, attached at Ex. A. As explained below and in the

Declaration of David A. Browne, attached hereto at Exhibit B, there is clearly good cause for the order.

One critical risk from unprotected disclosure of the documents is identity theft — a national problem that has attracted the attention of Congress, the President, and the FTC, as well as widespread media attention. Armed with information about the inner workings of Experian's system, identity thieves might be able to gain unauthorized access to the credit information concerning millions of consumers. *See* Declaration of David A. Browne ("Browne Decl."), Ex. B, ¶ 50. They might also be able to use the information to hide evidence of their crimes from their victims, who often detect the identity theft by observing the imposter's activity on their credit reports. This danger has grown all the more serious with the rise of well-funded and sophisticated criminal syndicates specializing in identity theft. Those syndicates would undoubtedly use information concerning Experian's system to further their crimes against consumers.

Another critical danger from the unprotected production of the documents is the loss of Experian's competitive advantage. *See id.* ¶¶ 48-49. Information about the structure, logic, and codes of Experian's system is invaluable to anyone attempting to reverse engineer the system. Experian's competitors and companies hoping to enter the credit reporting industry could build or refine a competing system at a small fraction of the costs incurred by Experian. They would unfairly receive the benefits of Experian's investment and hard work, without having to incur the costs.

For these and other reasons, there is good cause for the Proposed Protective Order and the other protections discussed below.

BACKGROUND

A. Experian Reports Credit Information Originated by Others.

Experian is a consumer credit reporting agency governed by the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq*. Experian collects credit information on more than 200 million consumers that is originated by others, such as information about the balances on a consumer's credit card accounts. Experian provides that information to parties for credit-related transactions. Experian does not make loans, decide who should receive credit, or set loan terms.

Experian has invested huge sums of money and countless hours of employee time to develop its unique and sophisticated computer system. That system gives Experian a major advantage in the highly competitive credit reporting marketplace. *See* Browne Decl., ¶ 47. Experian diligently guards against disclosure of information relating to the system. Among other things, Experian has introduced a number of safeguards, including the addition of an information security department within Experian. Experian also restricts access to sensitive documents within its own walls. In fact, documents containing secret information, such as the information at issue here, are given confidential status at Experian. Access to this information is permitted only to a select few employees who have an absolute need to know. *See id.*

B. The National Problem Of Consumer Identity Theft.

Identity theft is a crime in which an imposter obtains a consumer's personal information in order to "take over" the victim's existing credit accounts, to open new accounts in the victim's name, or to buy goods and services in the victim's name. The problem of identity theft has become front-page news, attracting the attention of Congress, the President, and federal regulators. In 2005, the Chairman of the FTC testified before a U.S. Senate Committee that nearly 10 million people were victims of identity theft in a recent one-year period. *See* Federal Trade Commission release, "FTC Testifies on Data Security and Identity Theft," (March 10,

2005), attached at Ex. C.[1] In July 2004, President Bush announced that identity theft cost the nation's businesses nearly $50 billion due to fraudulent transactions in 2003. *See* Remarks by President Bush at Signing of Identity Theft Penalty Enhancement Act (July 15, 2004), attached at Ex. D.[2] The identity theft problem has grown even more serious with the emergence of organized crime syndicates who engage in identity theft on a massive scale. Those syndicates actively seek to obtain information about how to circumvent Experian's system, hoping to learn information about potential victims or how to hide evidence of their crimes. As explained below, identity thieves could use the documents at issue here to steal the credit information of millions of consumers or to hide their crimes.

C. The Danger Posed By Competitors Or Potential Rivals.

Experian is part of the highly competitive consumer credit reporting industry. Experian competes with two other national credit reporting agencies and faces competition from numerous regional competitors, some of which are working toward becoming national credit reporting agencies. As discussed below, Experian's competitors could use information about Experian's system to update their own systems, thus destroying or eroding the business advantage that Experian has spent many years and millions of dollars creating. *See* Browne Dec., ¶ 47.

D. The Confidential Documents at Issue

(1) Documents Containing Confidential Codes & Information Specific to Plaintiff

Four of the documents requested by Plaintiff include Plaintiff's personal identifying information. These are the: (1) Administrative Report; (2) Dispute Response (or "D/R") Log; (3)

[1] *See* http://www.ftc.gov/opa/2005/03/idthefttest.htm.

[2] *See* http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html.

Disclosure Request Log; and (4) Transaction Logs (collectively, the "Confidential Code Documents").

The Administrative Report. The Administrative Report is a coded document generated by Experian's system. This internal report contains information that is not included in the credit reports Experian provides to third parties, nor in the file disclosures Experian has previously provided to Plaintiff. It is not created in the normal course of business, but is generated from Experian's computer systems for research regarding a specific consumer. Only a very limited number of trained Experian employees may create an Administrative Report. The Administrative Report at issue here was generated in response to Plaintiff's filing of this lawsuit. *See* Browne Decl., ¶¶ 5-8.

Confidential system codes appear throughout Plaintiff's Administrative Report. These codes include: (1) a confidential personal identification number (or PIN) which is unique to Plaintiff and is generated by Experian's system using Plaintiff's personal identifying information as reported to Experian and existing in Experian's consumer credit database; (2) confidential computer-generated "Name" and "Address" codes; (3) demographic information, whose codes reflect when information was reported to Experian and by whom; (4) coded social security information; (5) coded tradeline information for 46 tradelines including the creditor, balance date, monthly payment amount, payment level, account condition, payment status, Experian's internal subscriber number, the kind of business code, the type of account, the terms of credit, the Equal Credit Opportunity Act designation, the account open date, the actual amount of the last payment, any present delinquency, the maximum credit amount, a coded 13-month payment history, the account number, the last payment date, the number of months reviewed, and the number of previous delinquencies; (6) indicators reflecting whether each tradeline will or will

not be displayed on a credit report to a third party or on a disclosure to a consumer; and (7) a list of inquiries, including, *inter alia*, a code representing the type of permissible purpose the inquiring party had in accessing the file. *See id.* ¶¶ 9-23.

The Dispute Response Log. The "Dispute Response Log" ("D/R Log") is the second category of Confidential Code Documents that Experian seeks to protect. Here, one document is in this category. Like the Administrative Report, the D/R Log is not provided to consumers or to third parties who request a consumer's credit information. Nor is it generated in the ordinary course of business. The D/R Log is used for research purposes and may be generated only by a very limited number of trained Experian employees. *See id.* ¶¶ 24-26.

Confidential codes appear throughout Plaintiff's D/R Log. These include the confidential personal identification number (or PIN) unique to Plaintiff, the confidential computer-generated "Name" and "Address" codes, coded identifying and update information pertaining to Plaintiff's disputed tradeline, and a report, or "CAPID," number generated by Experian's computer system when Plaintiff's dispute was entered. *See id.* ¶¶ 27-32.

Disclosure Request Log. The third category of Confidential Code Documents that Experian seeks to protect is the "Disclosure Request Log." One Disclosure Request Log pertains to Plaintiff in this case. Like the other Confidential Code Documents, the Disclosure Request Log is not provided to consumers or to third parties who request a consumer's credit history information. The Disclosure Request Log can be generated from Experian's computer systems only by a very limited number of trained Experian employees, and they are used for research purposes regarding a specific consumer. Here, Experian generated the Disclosure Request Log at issue to investigate Plaintiff's disputes and in response to the Plaintiff's lawsuit. *See id.* ¶¶ 33-35.

The confidential codes appearing in Plaintiff's Disclosure Request Log includes the confidential personal identification number (or PIN) unique to Plaintiff and the report, or "CAPID," numbers generated by Experian's computer system each time a disclosure was requested. *See id.* ¶¶ 36-37.

Transaction Log. The Transaction Log is the final category of Confidential Code Documents that Experian seeks to protect. In this case, two documents fall within this category. Like the other Confidential Code Documents, the Transaction Logs are not provided to consumers or to third parties who request a consumer's credit information. Nor are they generated in the ordinary course of business. The Transaction Logs are used for research purposes and can be generated only by a very limited number of trained Experian employees. Experian generated Plaintiff's Transaction Logs after this action was filed. *See id.* ¶¶ 38-40.

Confidential codes appear throughout Plaintiff's Transaction Logs. These codes include: (1) the confidential personal identification number (or PIN) unique to Plaintiff; (2) coded Experian agent identification information; (3) a control number, generated by Experian's system each time a subscriber (*e.g.*, a credit grantor) requests that Experian update, delete, or otherwise change information related to a specific tradeline for reasons other than a consumer's dispute with Experian; and (4) additional codes identifying consumers, subscribers, tradelines, and the history of updates or changes made to a particular tradeline at the subscriber's request. *See id.* ¶¶ 41-44.

Each of the codes appearing in the four categories of Confidential Code Documents is integral to Experian's system. *See id.* ¶ 45. These documents are specific to Plaintiff and have not been produced in any prior litigation or provided to anyone outside Experian and its counsel.

See id. ¶¶ 8, 26, 35, 40. Experian strives to avoid producing these documents without a demarcation of confidentiality.

(2) Confidential Internal Policy and Procedure Manuals

Plaintiff has also requested certain documents identified collectively as the "Confidential Policy and Procedure Manuals." Specifically, Plaintiff demands the Consumer Investigation Procedures Participant Guide and the Mixed File Procedures Participant Guide.

Experian seeks to protect the Confidential Policy and Procedure Manuals. These documents contain proprietary information explaining how Experian maintains its credit reporting procedures. If publicly disclosed, these documents would provide the reader with a "road map" for circumventing Experian's policies and procedures, designed to assure maximum possible accuracy of consumer credit information. They would also enable current or potential competitors to enhance or develop a rival system, benefiting from the decades of work and millions of dollars that Experian has invested in its technology. The Consumer Investigation Procedures Participant Guide explains Experian's detailed procedures for handling every type of dispute that might arise, including numerous screen shots showing exactly what appears on the computer screen when an Experian employee processes a consumer's dispute. Similarly, the Mixed File Procedures Participant Guide contains screen shots throughout, showing exactly what appears on the computer screen when an Experian employee processes a consumer's dispute regarding a mixed file. The Mixed File Procedures Participant Guide also contains sensitive information about Experian's proprietary "do not combine" feature, including information about the design and operation of Experian's computer system.

Because of the highly proprietary information contained in the Policy and Procedure Manuals, Experian strives to protect these documents and avoids producing them without a demarcation of confidentiality. *See id.* ¶ 52.

STANDARD FOR ISSUANCE OF A PROTECTIVE ORDER

The Federal Rules of Civil Procedure empower this Court to issue protective orders "which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." *See* Fed. R. Civ. P. 26(c). This rule permits district courts "to issue protective orders constraining -- in any of a variety of ways -- the release of sensitive information." *Pearson v. Miller*, 211 F.3d 57, 72 (3d Cir. 2000). As the Third Circuit has held, a protective order should be entered where the party seeking the order shows good cause by demonstrating a particular need for protection. A showing of good cause requires the party seeking confidential treatment of the documents or information at issue to describe the injury with specificity. *See id.* at 72 -73 (citing cases); *Glenmede Trust Co. v. Thompson*, 56 F.3d 476, 483 (3d Cir. 1995) ("Good cause is established when it is specifically demonstrated that disclosure will cause a clearly defined and serious injury."). In appropriate circumstances, a district court may issue an umbrella protective order to protect a class of documents after a threshold showing by the party seeking protection. *See Pearson*, 211 F.3d at 73.

ARGUMENT

A. There Is Good Cause For A Protective Order As To The Confidential Code Documents.

The unprotected production of the Confidential Code Documents creates the risk that identity thieves would be able to gain unauthorized access to the credit histories of millions of consumers or to hide evidence of their crimes. In fact, disclosure of the documents would also heighten the risk that *Plaintiff's* identity would be stolen. The Confidential Code Documents

contain Plaintiff's full name, social security number, address, telephone number, and credit information.

The unprotected production of the documents also creates a serious risk that Experian's current and would-be competitors might be able to reverse engineer Experian's unique system, thus destroying Experian's competitive advantage and receiving the benefits of Experian's huge investment for free. *See* Browne Decl., ¶¶ 48-49. The Confidential Code Documents reveal highly confidential, proprietary information about the design and architecture of Experian's vast database. Experian's competitors could use that information to upgrade their systems. *See id.* Each additional internal report is a new picture that would provide new clues to the rules of Experian's matching system and Experian's design architecture overall.[3]

Experian will suffer serious, irreversible harm if the Confidential Code Documents are publicly disclosed. Thus, Experian has good cause for requesting this protective order. *See Pearson*, 211 F.3d at 73. Moreover, Experian does not seek to restrict Plaintiff's use of the information in this litigation, but only seeks to restrict its use for purposes unrelated to and outside this litigation. Accordingly, Plaintiff will not suffer any prejudice by the entry of this Order. *See In re Remington Arms Co., Inc.*, 952 F.2d 1029, 1033 (8th Cir. 1991).

B. There Is Good Cause For A Protective Order As To The Policy And Procedure Manuals.

As with the Confidential Code Documents, the unprotected disclosure of the Confidential Policy and Procedure Manuals create serious risks of identity theft and reverse engineering. The Consumer Investigation Procedures Participant Guide explains Experian's detailed procedures for handling every type of dispute that might arise, including numerous screen shots showing

[3] It is not enough simply to redact codes from these reports. The very structure of the information on these reports, in conjunction with all of the identifying information about a consumer, reveals information about the variables integrated into Experian's sophisticated matching system and reflects the trade secrets of how Experian's computer systems work.

exactly what appears on the computer screen when an Experian employee processes a consumer's dispute. Similarly, the Mixed File Procedures Participant Guide contains screen shots throughout, showing exactly what appears on the computer screen when an Experian employee processes a consumer's dispute regarding a mixed file. The Mixed File Procedures Participant Guide also contains sensitive information about Experian's proprietary "do not combine" feature, including information about the design and operation of Experian's computer system.

The confidentiality of Experian's Confidential Policy and Procedure Manuals is necessary to protect consumers. Disclosure of the manuals would show identity thieves how Experian's system works, creating a high risk that those individuals would be able to develop methods to circumvent Experian's procedures. Ultimately, this would damage the integrity of the credit reporting industry, making it more difficult for consumers who pay their bills on time to obtain credit. *See* Browne Decl., ¶¶ 59-60. Disclosure also would threaten Experian's competitive advantage, for Experian's competitors would benefit substantially by gaining access to information regarding Experian's system. *See id.* ¶¶ 55-56.

As with the Confidential Code Documents, Experian will suffer serious, irreversible harm if the Confidential Policy and Procedure Manuals are disclosed without benefit of a protective order. Accordingly, the good cause requirement has been satisfied and the Proposed Protective Order should be entered. *See Pearson*, 211 F.3d at 72-73.

C. Protections Sought for Categories of Documents

The Third Circuit has affirmed the district courts' discretion to impose any of a variety of methods for protecting confidential information. *See Pearson*, 211 F.3d at 73 ("Rule 26(c) provides district courts with the power to formulate a detailed solution that reflects the concerns of particular individual disputes."). Thus, this court may enter a protective order that

encompasses "any of a broad range of requirements," including: (1) the "terms and conditions" pursuant to which disclosure may be arranged; (2) that the scope of the disclosure be "limited to certain matters"; and (3) that disclosure "be conducted with no one present except persons designated by the court." *Id.*

In this case, Plaintiff's counsel seeks these documents for purposes of deposing Experian witnesses and to evaluate this matter for settlement. *Cf. Pansy v. Borough of Stroudsburg*, 23 F.3d 772, 788 (3d Cir. 1994) ("[I]f a case involves private litigants, and concerns matters of little legitimate public interest, that should be a factor weighing in favor of granting … an order of confidentiality."). By agreeing to Experian's Stipulated Protective Order, in this case and others, Plaintiff's counsel has demonstrated his agreement that confidential treatment of these documents is appropriate. Indeed, Plaintiff's counsel's only recent challenge to confidential treatment of these documents was heard and rejected in 2005. *See Vidal v. Experian Information Solutions, Inc.*, E.D. Pa. No. CV-04-3867 (order granting Experian's motion for protective order because "there would be a competitive disadvantage to Experian if these documents were in the public domain") (entered Feb. 3, 2005), attached at Ex. E.[4]

(1) Confidential Treatment Should Be Granted For The Administrative Report, D/R Log, Disclosure Request Log, and Transaction Logs

In prior cases, Experian has designated each of these documents as "Confidential" and produced them to parties upon the entry of an appropriate protective order. Experian also has requested, and courts have entered orders endorsing, the following protective measures for these documents: (1) to the extent that any motions, briefs, pleadings, deposition transcripts, or other papers to be filed with the Court incorporate these documents, the party filing such papers shall

[4] In the *Vidal* matter, only the Administrative Report, Dispute Response Log, Disclosure Request Log, and Transaction Logs were at issue.

do so under seal and designate such materials, or portions thereof, as "Confidential;" (2) the documents shall not be used for any business, commercial or competitive purposes, or for *any* purpose other than the preparation and trial of that lawsuit; (3) the documents shall not be disclosed to any person other than the Court and its officers, parties to the litigation, counsel for the parties, fact witnesses who need the information, and Experian employees without Experian's prior written consent; and (4) all documents shall be returned to Experian within 60 days of the end of the litigation.

As noted above, these documents contain not only confidential codes that could be of use to those attempting to reverse engineer or "to compromise" Experian's consumer credit database, but also Plaintiff-specific information that could be used to steal Plaintiff's identity. Accordingly, Experian seeks the protections granted by courts in previous cases for these four documents.

(2) Confidential Treatment Sought for Relevant Portions of Consumer Investigation Procedures Participant Guide

In the past, Experian has produced only those portions of the Consumer Investigation Procedures Participant Guide relevant to the issues in the particular case. Each produced page has been clearly marked "Confidential." Accordingly, Experian seeks to produce only those portions of the Consumer Investigation Procedures Participant Guide related to the topics at issue in this case. The remainder of the document, which is more than 400 pages long, is wholly irrelevant to the Plaintiff's claim -- and, consequently, to any issues that might legitimately arise in settlement discussions. In addition, Experian requests an Order permitting it to provide Plaintiff with the relevant portions of the Consumer Investigation Procedures Participant Guide pursuant to the four protective measures listed in conjunction with the four Confidential Code Documents discussed in section (1). *See supra*, section C(1).

(3) Confidential Treatment Sought for Mixed File Procedures Participant Guide

For the reasons listed above, Experian seeks to produce the Mixed File Procedures Participant Guide pursuant to the four protective measures listed in conjunction with the four Confidential Code Documents discussed in section (1). *See supra*, section C(1). Because this case is premised upon a "mixed file," Experian is willing to produce the Mixed File Procedures Participant Guide in its entirety, with each page clearly marked "Confidential."

CONCLUSION

Experian has complied with all deadlines in this matter and is merely seeking to enforce its long-standing policy of not producing confidential documents containing proprietary, trade secret information, until and unless an appropriate protective order is in place. Good cause exists for this Court to enter the Proposed Protective Order attached at Exhibit A. Accordingly, Experian respectfully requests that Experian's Motion for Protective Order be granted.

Dated: December 3, 2007

Respectfully submitted,

/s/ Mohammad A. Ghiasuddin
Mohammad A. Ghiasuddin
Kaplin Stewart Meloff Reiter & Stein
350 Sentry Parkway
Building 640, P.O. Box 3037
Blue Bell, PA 19422-0765
(610) 260-6000

Neelie S. Simmons
Jones Day
500 Grant Street, Suite 3100
Pittsburgh, PA 15219
(412) 391-3939

Counsel for Defendant
EXPERIAN INFORMATION SOLUTIONS, INC.

EXHIBIT A

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SANDRA M. RINEER,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	**Civil Action No. 07-3739**
	)	
EXPERIAN INFORMATION SOLUTIONS, INC.,	)	
	)	
	)	
Defendant.	)	

PROPOSED PROTECTIVE ORDER

WHEREAS, documents and information in the custody and control of Defendant Experian Information Solutions, Inc. ("Experian") have been sought by Plaintiff; and

WHEREAS, these documents relate to trade secrets, confidential research, development, technology or other proprietary information belonging to Experian; and

WHEREAS, Experian has shown good cause for confidential treatment of these documents and the information contained therein;

THEREFORE, an Order of this Court protecting such confidential information shall be and hereby is made by this Court on the following terms:

1. This Order shall govern the use, handling and disclosure of the following categories of documents generated by Experian Information Solutions, Inc. ("Experian") in response to the instant lawsuit: 1) the Administrative Report; 2) the Dispute Response (or "D/R") Log; 3) the Disclosure Request Log; and 4) the Transaction Logs (collectively, the "Confidential Code Documents"). Additionally, this Order shall govern the use, handling and disclosure of the Consumer Investigation Procedures Participant Guide and the Mixed File Procedures Participant Guide (collectively, the "Confidential Policy and Procedure Manuals").

This Order shall further govern the use of any testimony, materials or other information regarding the highly confidential internal codes and other information contained in the Confidential Code Documents and in the Confidential Policy and Procedure Manuals.

2. All parties to this case shall treat as confidential the Confidential Code Documents and the Confidential Policy and Procedure Manuals and all transcripts and other materials that reflect or incorporate the confidential information therein. Specifically, the parties shall proceed as follows:

a) Any party or non-party producing or filing the Confidential Code Documents or the Confidential Policy and Procedure Manuals in this action may designate such materials and the information contained therein subject to this Order by typing or stamping on the front of the document, or on the portion(s) of the document for which confidential treatment is designated, "Confidential."

b) To the extent any motions, briefs, pleadings, deposition transcripts, or other papers to be filed with the Court incorporate the Confidential Code Documents, the Confidential Policy and Procedure Manuals, or other testimony or information subject to this Order, the party filing such papers shall designate such materials, or portions thereof, as "Confidential" and shall file them with the clerk under seal; provided, however, that a copy of such filing having the confidential information deleted therefrom may be made part of the public record.

c) The Confidential Code Documents, Confidential Policy and Procedure Manuals, and other materials or information revealing the confidential content of those documents (including, but not limited to, all testimony, deposition, or

otherwise, that refers, reflects or otherwise discusses any information designated "Confidential,") shall not be used, directly or indirectly, by any person (including other defendants) for any business, commercial or competitive purposes or for any purpose whatsoever other than solely for the preparation and trial of this action in accordance with the provisions of this Order.

d) Except with the prior written consent of the individual or entity asserting confidential treatment, or pursuant to prior Order after notice, any document, transcript or pleading marked as "Confidential" under this Order, and any information contained in, or derived from any such materials (including, but not limited to, all testimony, deposition or otherwise, that refers, reflects or otherwise discusses any information designated confidential hereunder), may not be disclosed other than in accordance with this Order and may not be disclosed to any person other than: (a) the Court and its officers; (b) parties to this litigation; (c) counsel for the parties, whether retained counsel or in-house counsel and employees of counsel assigned to assist such counsel in the preparation of this litigation; (d) fact witnesses subject to a proffer to the Court or a stipulation of the parties that such witnesses need to know such information; and (e) present or former employees of the producing party in connection with their depositions in this action (provided that no former employees shall be shown documents prepared after the date of his or her departure).

e) All persons receiving any or all Confidential Code Documents or Confidential Policy and Procedure Manuals produced pursuant to this Order shall be advised of their confidential nature. All persons to whom Confidential Code Documents, Confidential Policy and Procedure Manuals, and/or information contained in, or derived from any such materials, are disclosed are hereby enjoined from disclosing same to any other person except as provided herein, and are further enjoined from using same except in the preparation for and trial of the above-captioned action between the named parties thereto. No person receiving or reviewing such Confidential Code Documents, Confidential Policy and Procedure Manuals, information or transcript shall disseminate or disclose them to any person other than those described above in Paragraph 6(d) and for the purposes specified, and in no event shall such person make any other use of such document or transcript.

3. Nothing in this Order shall prevent a party from using at trial any Documents, information or materials designated "Confidential."

4. This Order has been entered to facilitate discovery and the production of relevant evidence in this action. Neither the entry of this Order, nor the designation of any information, document, or the like as "Confidential," nor the failure to make such designation, shall constitute evidence with respect to any issue in this action.

5. Within sixty (60) days after the final termination of this litigation, all Confidential Code Documents, Confidential Policy and Procedure Manuals, transcripts and other materials afforded confidential treatment pursuant to this Order, including any extracts, summaries or compilations taken therefrom, but excluding any materials which in the good faith

judgment of counsel are work product materials, shall be returned to the individual or entity having produced or furnished same.

6. In the event that any party to this litigation disagrees at any point in these proceedings with any designation made under this Protective Order, the parties shall first try to resolve such dispute in good faith on an informal basis. If the dispute cannot be resolved, the party objecting to the designation may seek appropriate relief from this Court. During the pendency of any challenge to the designation of a document or other information, the designated document or information shall continue to be treated as "Confidential" subject to the provisions of this Protective Order.

7. Nothing herein shall affect or restrict the rights of any party with respect to its own documents or to the information obtained or developed independently of documents, transcripts and materials afforded confidential treatment pursuant to this Order.

IT IS SO ORDERED.

Dated: _____

_____
UNITED STATES DISTRICT JUDGE

EXHIBIT B

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

SANDRA M. RINEER,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	**Civil Action No. 07-3739**
	)	
EXPERIAN INFORMATION SOLUTIONS, INC.,	)	
	)	
	)	
Defendant.	)	

DECLARATION OF DAVID A. BROWNE

I, David A. Browne, being duly sworn, declare and state as follows:

I. Background

1. Since 1996, I have served as Compliance Manager for Experian Information Solutions, Inc. ("Experian"), formerly known as the Information Services Division, TRW Information Systems Group, of TRW Inc. Before that time, I held the same position with TRW in its Information Services Division. I joined TRW Inc. ("TRW") as a system analyst in January 1977, and during my employment with TRW my assignments included redesigning TRW's credit report and adding information to it as well. I also tested some of the changes to the computer system and developed the business rules for some of the changes. I have additionally identified and specified a number of enhancements to the computer systems and procedures used by TRW and Experian over the past 16 years. My current duties include helping to ensure that Experian's computer systems and procedures comply with federal and state credit reporting laws and Experian's requirements for quality. I am fully familiar with the procedures that Experian employs in gathering and storing credit information and in assembling credit reports and consumer disclosures.

2. Based upon my experience at Experian, I am very familiar with Experian's policies and procedures for the compilation, retention, reinvestigation and disclosure of consumer credit information. The facts set forth herein are based upon my personal knowledge, and if I were called upon to testify to them, I could and would competently do so.

3. I submit this affidavit in support of Experian's Motion for Protective Order in the above-captioned matter.

4. Plaintiff seeks to discover certain documents in Experian's possession. These documents are identified as the Administrative Report, the Dispute Response (or "D/R") Log, the Disclosure Request Log, and the Transaction Log (collectively, the "Confidential Code Documents") pertaining to Plaintiff. Plaintiff also seeks to discover the Consumer Investigation Procedures Participant Guide and the Mixed File Procedures Participant Guide (collectively, the "Confidential Policy and Procedure Manuals").

II. The Four Confidential Code Documents at Issue

A. Administrative Report

5. Inquiry/Generation. The first Confidential Code Document Experian seeks to protect is an Administrative Report. This nineteen-page Report was generated on October 16, 2007, at the request of Experian's counsel. The Report was generated to assist Experian's research and investigation into Plaintiff's claims.

6. The Report is specific to Plaintiff. It consists of a coded depiction of Plaintiff's identifying and credit information as it currently exists in Experian's consumer credit database, as well as certain historical reporting of Plaintiff's identifying and credit information.

7. Plaintiff's Administrative Report is not part of the credit reports Experian provides to third parties, nor is it part of the file disclosures Experian provides to consumers.

The Administrative Report is not created in the normal course of business, but is generated from Experian's computer systems for a specific consumer. The Administrative Report is used by Experian for research purposes and may be generated only by a very limited number of trained Experian employees.

8. Experian generated the Administrative Report pertaining to Plaintiff after Plaintiff filed this lawsuit against Experian. The Administrative Report did not previously exist, though the information contained in the Administrative Report was stored in Experian's computer systems. The specific Administrative Report sought by Plaintiff has not been produced in any prior litigation or provided to anyone whatsoever outside Experian and its counsel.

9. The Report begins with the inquiry input line, *i.e.*, a code for the Experian employee requesting the report and the identifying information of Plaintiff used to create the report. The next line includes the page number of the Report, the date it was generated, and a code for the Experian office from which the Report was generated.

10. Confidential PIN. The Report continues with Experian's computer-generated confidential PIN or personal identification number. This number is unique to Plaintiff and is generated by Experian's computer system based on the basket of Plaintiff's personal identifying information as reported to Experian and existing in Experian's consumer credit database. The PIN represents Plaintiff's information and the location of that information in Experian's consumer credit database.

11. Confidential "Name" Codes. Next, the Report lists the variations of Plaintiff's name and social security number as reported to Experian, and coded information representing the time periods those name and social security number variations were reported to Experian. Experian's computer system gives each such variation a unique "Name" code.

12. The Report at issue contains fourteen different "Name" variations, each with a computer-generated code, and each including coded information regarding when that variation was reported to Experian. The "Name" variations are culled from public record information, credit and loan account information (referred to as "trade lines") as well as inquiries into Plaintiff's Experian file.

13. The coded "Name" variations were generated by Experian's computer system for Experian's internal use, have never been disclosed before, and do not appear in any credit reports to third parties or in any consumer file disclosure sent to Plaintiff. These name codes re-appear throughout the Report, identifying which "Name" variation was reported to Experian for the specific trade line or inquiry listed. The actual name variations themselves (without the confidential, computer-generated code) appear as an "aka" on credit reports to third parties and are disclosed on consumer file disclosures sent to the consumer.

14. Other Coded Identifying and Internal Information. After the coded "Name" variations is a row of other identifying information and Experian indicators. This row generally includes date of birth information, spouse information, when such information was reported, and other indicators such as whether Experian has instituted certain additional procedures when multiple consumer files are mixed into one.

15. Confidential "Address" Codes. The next set of information on the Report lists the variations of Plaintiff's address as reported to Experian, and coded information representing the time periods the address variations were reported to Experian. Like the "Name" code, Experian's computer system gives each address variation a unique "Address" code.

16. The Report at issue contains five "Address" variations, each with a computer-generated code, and each including coded information regarding when that variation was

reported to Experian. The "Address" variations, like the "Name" variations, are culled from public record information, credit and loan account information (referred to as "trade lines") as well as inquiries into Plaintiff's Experian file.

17. The coded "Address" variations were generated by Experian's computer system for Experian's internal use, have never been disclosed before, and do not appear in any credit reports to third parties or in any consumer file disclosure sent to Plaintiff. These address codes re-appear throughout the Report, identifying which "Address" variation was reported to Experian for the specific trade line or inquiry listed. The actual address variations themselves (without the confidential, computer-generated code) appear as additional addresses on credit reports to third parties and are disclosed on consumer file disclosures sent to the consumer.

18. Demographics. The next set of information is demographic information, again coded to reflect who reported the information and when the information was reported to Experian. Here, Plaintiff's Report includes the GEO code of Plaintiff's current address. (The GEO code is the Census Bureau's code containing the state, Metropolitan Statistical Area, county, tract and block group of the address at issue.) Decoded demographic information may appear on credit reports to third parties and are disclosed on consumer file disclosures sent to the consumer.

19. FACS + Summary. The next set of information is titled the "FACS+ Summary." ("FACS" stands for "file address check service".) This section includes when the input social security number was issued, the United States Post Office standardization as to the type of address, *e.g.*, residential, military, etc. Decoded information may appear on credit reports to third parties and are disclosed on consumer file disclosures sent to the consumer.

20. Confidential Computer-Coded Information for Trade Display. Following the "FACS+ Summary" on the Report is the tradeline information. The Report contains forty-six tradelines.

21. Each trade line contains coded information including the subscriber (creditor), balance date, monthly pay amount, payment level, account condition, payment status, Experian's internal subscriber number, the kind of business code, the type of account, the term of credit, the Equal Credit Opportunity Act designation, the account open date, the actual amount of the last payment, any present delinquency, the maximum credit amount, a coded 13-month payment history, the account number, the last payment date, any previous delinquency, the number of months reviewed, the number of 30-day, 60-day, 90-day or other delinquencies. This information appears on credit reports to third parties and is presented in an easy-to-read, plain English format on consumer file disclosures sent to the consumer.

22. Trade Information and Confidential "Name" and "Address" Codes. Along with this information, for each trade line is additional balance information, Experian's confidential computer-generated "Name" and "Address" codes, and a series of additional codes summarizing information reported to Experian as well as other indicators reflecting whether the specific tradeline at issue will or will not be displayed on a credit report to a third party or on a disclosure to a consumer. This information does not appear on credit reports to third parties and does not appear on consumer file disclosures sent to the consumer. Rather, this information is used by Experian's complex computer system to match the specific tradeline to the consumer, and is the input information upon which the computer system relies to process and display the trade information on both credit reports and file disclosures.

23. Inquiries and Confidential "Name" and "Address" Codes. The last set of information is a list of inquiries into Plaintiff's Experian file. The inquiries list the name of the inquiring party, the date of the inquiry, Experian's internal subscriber number or business number, and, for most inquiries, a code representing the type of permissible purpose the inquiring party had in accessing the file. For inquiries by Experian, most often the entry includes an internal reference number to correspond with a disclosure sent to the consumer, or an investigation conducted at the request of the consumer. Finally, each inquiry lists the confidential, computer-generated "Name" and "Address" codes used in making the credit inquiry.

B. Dispute Response Log ("D/R" Log)

24. Inquiry/Generation. The second type of Confidential Code Document Experian seeks to withhold in this particular case, absent a protective order, is Ms. Rineer's Dispute Response (or "D/R") Log. The D/R Log was generated on October 16, 2007. The D/R Log was generated for investigative and research purposes only, and contains numeric and alphabetical codes, similar to those contained in Ms. Rineer's Administrative Report, throughout.

25. Plaintiff's D/R Log is not part of the credit reports Experian provides to third parties, nor is it part of the file disclosures Experian provides to consumers. The D/R Log is generated from Experian's computer systems for a specific consumer. The D/R Log is used by Experian for research purposes and may be generated only by a very limited number of trained Experian employees.

26. The D/R Log did not exist prior to Experian's investigations, though the information contained in the D/R Log was stored in Experian's computer systems. The specific

D/R Log sought by Plaintiff has not been produced in any prior litigation or provided to anyone whatsoever outside Experian and its counsel.

27. Confidential PIN. Ms. Rineer's D/R Log consists of twenty pages containing confidential information including an internal PIN. This number is unique to Plaintiff and is generated by Experian's computer system based on the basket of Plaintiff's personal identifying information as reported to Experian and existing in Experian's consumer credit database. The PIN represents Plaintiff's information and the location of that information in Experian's consumer credit database.

28. Confidential "Name" Codes. Next, the Log contains a unique "Name" code. The coded "Name" was generated by Experian's computer system for Experian's internal use, has never been disclosed before, and does not appear in any credit reports to third parties or in any consumer file disclosure sent to Plaintiff.

29. Confidential "Address" Codes. An address code also produced by Experian's system appears in Plaintiff's D/R Log as well. Like the "Name" code, Experian's computer system gives each address variation a unique "Address" code. The coded "Address" has never been disclosed before, and does not appear in any credit reports to third parties or in any consumer file disclosure sent to Plaintiff.

30. Agent Codes. Coded Experian agent identification information also appears in the D/R Log. This information does not appear in any credit reports to third parties or in any consumer file disclosure sent to Plaintiff.

31. Trade Information and Confidential "Name" and "Address" Codes. Coded identifying and update information pertaining to Ms. Rineer's disputed tradeline appears in the D/R Log. Balance information, Experian's confidential computer-generated "Name" and

"Address" codes, dispute information and a series of additional codes summarizing information reported to Experian also appear. This information does not appear on credit reports to third parties and does not appear on consumer file disclosures sent to the consumer. Rather, this information is used by Experian's complex computer system to match the specific tradeline to the consumer, and is the input information upon which the computer system relies to process and display the trade information on both credit reports and file disclosures.

32. Report (or "CAPID") Number. A CAPID number was produced by Experian's system when a disclosure was created. This number was generated for internal use only, has never been produced before, and does not appear in any credit report to third parties or in any consumer file disclosure sent to Ms. Rineer.

C. Disclosure Request Log

33. Inquiry/Generation. The third type of Confidential Code Document Experian seeks to withhold in this particular case, absent a protective order, is Ms. Rineer's Disclosure Request Log. The Disclosure Request Log was generated in October 2007. The Disclosure Request Log was generated for investigative and research purposes only.

34. Plaintiff's Disclosure Request Log is not part of the credit reports Experian provides to third parties, nor is it part of the file disclosures Experian provides to consumers. The Disclosure Request Log is generated by Experian's computer systems for a specific consumer. The Disclosure Request Log is used by Experian for research purposes and may be generated only by a very limited number of trained Experian employees.

35. The Disclosure Request Log did not exist prior to Experian's investigations, though the information contained in the Disclosure Request Log was stored in Experian's computer systems. The specific Disclosure Request Log sought by Plaintiff has not been

produced in any prior litigation or provided to anyone whatsoever outside Experian and its counsel.

36. Confidential PIN. Ms. Rineer's Disclosure Request Log consists of two pages containing confidential information including Ms. Rineer's personal identifying information and an internal PIN. This number is unique to Plaintiff and is generated by Experian's computer system based on the basket of Plaintiff's personal identifying information as reported to Experian and existing in Experian's consumer credit database. The PIN represents Plaintiff's information and the location of that information in Experian's consumer credit database.

37. Report (or "CAPID") Number. A CAPID number was generated by Experian's system each time a disclosure was created. These numbers were generated for internal use only, have never been produced before, and do not appear in any credit report to third parties or in any consumer file disclosure sent to Ms. Rineer.

D. Transaction Log

38. Inquiry/Generation. The fourth type of Confidential Code Document Experian seeks to withhold in this particular case, absent a protective order, is Plaintiff's Transaction Logs. There are two Transaction Logs specific to Plaintiff; they were generated on October 17, 2007 and October 27, 2007 for investigative and research purposes only.

39. Plaintiff's Transaction Logs are not part of the credit reports that Experian provides to third parties, nor are they part of the file disclosures that Experian provides to consumers. The Transaction Logs are generated by Experian's computer systems for a specific consumer. The Transaction Logs are used by Experian for research purposes and may be generated only by a very limited number of trained Experian employees.

40. Experian generated these Transaction Logs pertaining to Plaintiff after Plaintiff filed this lawsuit against Experian. The Transaction Logs did not previously exist, although the information contained in the Transaction Logs was stored in Experian's computer systems. The specific Transaction Logs sought by Plaintiff have not been produced in any prior litigation or provided to anyone whatsoever outside Experian and its counsel.

41. Confidential PIN. Plaintiff's Transaction Logs consist of eight pages and contain confidential information, including Plaintiff's personal identifying information and an internal PIN. This PIN is unique to Plaintiff and is generated by Experian's computer system based on the basket of Plaintiff's personal identifying information as reported to Experian and existing in Experian's consumer credit database. The PIN represents Plaintiff's information and the location of that information in Experian's consumer credit database.

42. Agent Codes. Coded Experian agent identification information also appears in the Transaction Logs. This information does not appear in any credit reports to third parties or in any consumer file disclosure sent to Plaintiff.

43. Control Number. A Control Number was generated by Experian's system each time a subscriber (*e.g.*, a credit grantor) requested that Experian update, delete, or otherwise change information related to a specific tradeline for reasons other than a consumer's dispute with Experian. These numbers were generated for internal use only, have never been produced before, and do not appear in any credit report to third parties or in any consumer file disclosure sent to Plaintiff.

44. Trade Information and Other Confidential Codes. The Transaction Logs also contain codes that identify consumers, subscribers, tradelines, and the history of updates or changes made to a particular tradeline at the subscriber's request. Account status information

and a series of additional codes summarizing information reported to Experian are also reported. This information does not appear on credit reports to third parties and is not included in consumer file disclosures sent to the consumer. Rather, this information is used by Experian's complex computer system to match the specific tradeline to the consumer and update, delete, or change the tradeline according to the subscriber's request.

III. Experian's Computer System is its Business

45. Each of the codes described in paragraphs 10 through 44 above is integral to Experian's credit reporting system, which is, in itself, confidential and proprietary. Experian maintains credit information on more than 200 million consumers. Experian has worked hard and has incurred great cost updating its computer hardware and software to create a credit-reporting system able to compile credit information and prepare credit reports assuring maximum possible accuracy of the information contained therein.

46. Experian's competitors would benefit substantially by gaining access to detailed information regarding Experian's computer hardware and software and the confidential, proprietary documentation that reflects the trade secrets of how Experian's computer systems work.

47. Experian's credit reporting computer system *is its business*. As such, Experian has designed a unique computer system to process information received from tens of thousands of diverse lenders and other entities involved in the credit industry, from the public record, and from other sources. Experian has spent millions of dollars and countless hours of employee time developing and enhancing its sophisticated computer system to achieve maximum possible accuracy of the credit information Experian provides to those with permissible purposes for receiving consumer credit information. By doing so, Experian enjoys a competitive advantage in

the credit reporting marketplace. Consequently, if information about its system were to get into the hands of a current or potential competitor, it would enable the competitor to create or enhance its own systems and remove the marketing edge currently enjoyed by Experian. Furthermore, if this information were to fall into criminal hands, it would threaten the credibility of Experian's entire credit reporting system and pose a serious threat to the privacy of consumers on whom Experian reports information. Such actions could lead to a loss of confidence in Experian's credit reports. Accordingly, Experian strives to maintain the secrecy of its computer systems, and access to this highly sensitive information is strictly limited only to those with an absolute need to know.

IV. Three Primary Risks of Disclosing Codes and Information Displayed

48. Risk of Reverse-Engineering. The first primary risk associated with production of these documents is the threat of reverse-engineering. The type, nature and manner of display of the information in the Confidential Code Documents sought by Plaintiff can be used to reverse-engineer Experian's matching system rules -- its "Crown Jewels" -- and to ultimately erode Experian's competitive advantage. Experian has spent substantial sums of money over many years to develop a method of matching consumer information. The specific details of this matching system are not voluntarily or intentionally disclosed in lawsuits or to any government agency.

49. Someone seeking to reverse-engineer Experian's matching system would find the codes and coded information contained in these documents, as well as the structure of these documents, extremely useful. By comparing the type and nature of information included on multiple documents such as these, related to different consumers, a person could undertake to reverse-engineer Experian's matching system. Each additional document produced and made

public would have an incremental benefit to those who would copy Experian's matching system. Thus, the more examples of these documents that reach the public sphere, the greater their value to those who would copy or reverse-engineer Experian's system. Increased access to Experian's Confidential Documents therefore increases the probability that outsiders will be able to discern the "Crown Jewels" of Experian's credit reporting systems and procedures. Accordingly, Experian strives to protect these documents and to avoid producing them without a protective order.

50. Risk of Identity Theft. The second risk associated with producing these documents without benefit of a protective order is the risk of identity theft. These documents contain information that is unique to the Plaintiff: full name, social security number, address, telephone number, employment, and credit information. This information would be of great use to someone seeking to steal another's identity for his personal gain. Over time, the increased risk and incidence of identity theft may compromise the credit reporting system in general.

51. Risk of Interference from Credit Clinics. The third risk associated with producing the above-described documents is the potential for interference by unscrupulous credit clinics with Experian's consumer credit database. Armed with knowledge of Experian's match code information, such clinics could advise a consumer with poor credit on how to adjust his identifying information so as to lose his existing bad credit history and gain a fresh start at the expense of consumers who do pay their bills. In short, repeated, unprotected production of these documents ultimately would jeopardize the integrity of the credit reporting industry, making it more expensive and more difficult for consumers who pay their bills in a timely fashion to obtain credit.

VI. The Confidential Policy and Procedure Manuals

52. Plaintiff has also requested certain documents that are identified collectively as the "Confidential Policy and Procedure Manuals." Specifically, these documents are as follows: (1) the Consumer Investigation Procedures Participant Guide and (2) the Mixed File Procedures Participant Guide.

53. Experian seeks to protect its Confidential Policy and Procedure Manuals. These documents contain proprietary information on how Experian maintains its credit reporting procedures. The Consumer Investigation Procedures Participant Guide, for example, walks the reader through Experian's detailed procedures for handling every type of dispute that might arise, including numerous screen shots showing exactly what appears on the computer screen when an Experian employee processes a consumer's dispute. Similarly, the Mixed File Procedures Participant Guide contains screen shots throughout, showing exactly what appears on the computer screen when an Experian employee processes a consumer's dispute regarding a mixed file. The Mixed File Procedures Participant Guide also contains sensitive information about Experian's proprietary "do not combine" feature, including information about the design and operation of Experian's computer system.

A. The Confidentiality of Experian's Policy and Procedure Manuals is Necessary to Protect Experian's Competitive Position in the Credit Reporting Market.

54. Experian has invested very large sums of money and countless hours of employee time throughout the years developing and enhancing its sophisticated policies and procedures to achieve maximum possible accuracy and completeness of the credit information Experian provides to those with permissible purposes for receiving consumer credit information. By doing so, Experian enjoys a competitive advantage in the credit reporting marketplace.

55. Development of a highly accurate consumer credit reporting system involves delicate incorporation of accumulated knowledge -- knowledge which must, therefore, be protected from those who would seek to improve or develop a rival system by obtaining Experian's secrets, instead of investing as extensively as Experian has done over many years and continues to do so today.

56. In order to protect its system, Experian has introduced a number of safeguards, including the addition of an information security department within Experian, information security regulations, and mandatory information security training of all employees. Experian also restricts access to sensitive documents within its own walls. In fact, documents containing secret information, such as those presently at issue, are given confidential status at Experian. For example, the notation placed on each page of the Consumer Investigation Procedures Participant Guide and the Mixed File Procedures Participant Guide states that the document is "Confidential and Proprietary."

57. Experian's competitors would benefit substantially by gaining access to detailed information regarding Experian's computer software and the confidential, proprietary documentation that reflects the trade secrets of how Experian's computer systems and investigation procedures function. This detailed information is contained in the Confidential Policy and Procedure Manuals at issue.

58. Consequently, if information about its system were to fall into the hands of a current or potential competitor, it would enable the competitor to create or enhance its own procedures and remove the marketing edge currently enjoyed by Experian. Thus, in litigation matters, Experian vigorously strives to ensure that these documents are not produced without a Court-sanctioned protective order.

B. The Confidentiality of Experian's Policy and Procedure Manuals is Necessary to Protect Consumers.

59. Furthermore, if the information contained in Experian's Confidential Policy and Procedure Manuals were to fall into criminal hands, it would threaten the credibility of Experian's entire credit reporting system and pose a serious threat to all consumers on which Experian reports information. Such actions could lead to a loss of confidence in Experian's credit reports.

60. More importantly, however, permitting access to Experian's Confidential Policy and Procedure Manuals would open up Experian's system to potential criminals, making it easier for identity theft to take place, and making it more difficult to detect and remedy identity theft after it has taken place.

61. Disclosure of the Confidential Policy and Procedure Manuals to the public effectively shows potential criminals exactly how Experian's system works, creating a high risk that those individuals would be able to develop methods to successfully circumvent Experian's procedures.

62. Accordingly, Experian strives to protect these Confidential Policy and Procedure Manuals and avoids producing them without benefit of a protection order guaranteeing their confidentiality. As it has done in the past, Experian seeks to produce *only* those portions of the Consumer Investigation Policies and Procedures Guide relevant to the re-investigation at issue.

David A. Browne
Compliance Manager

STATE OF CALIFORNIA)
) SS:
COUNTY OF ORANGE)

On November 29, 2007, before me, NIKOLE L. MARASCO, a Notary Public, personally appeared David A. Browne, personally known to be the person whose name is subscribed to the within instrument and acknowledged to me that he executed the same in his authorized capacity, and that by his signature on the instrument the person, or the entity upon behalf of which the person acted, executed the instrument.

WITNESS my hand and official seal.

NIKOLE L. MARASCO
Commission # 1476791
Notary Public - California
Orange County
My Comm. Expires Mar 16, 2008

EXHIBIT C

Federal Trade Commission
Protecting America's Consumers

For Release: March 10, 2005

FTC Testifies on Data Security and Identity Theft

The Federal Trade Commission testified today before the U.S. Senate Committee on Banking, Housing, and Urban Affairs about the reach of existing federal laws that require certain information providers to safeguard sensitive information and to ensure that the information doesn't fall into the wrong hands. The Senate Banking Committee is examining recent developments involving the security of sensitive consumer information.

FTC Chairman Deborah Platt Majoras said that increased scrutiny about the security of consumer data takes place against the background of the threat of identity theft, a crime that harms both consumers and financial institutions. "A 2003 FTC survey showed that over a one-year period, nearly 10 million people – or 4.6 percent of the adult population – had discovered that they were victims of some form of identity theft."

There are three laws enforced by the FTC that restrict disclosure of consumer information and require companies to ensure the security and integrity of the data in certain contexts, the testimony says.

"The Fair Credit Reporting Act primarily prohibits the distribution of 'consumer reports' by 'consumer reporting agencies' (CRAs) except for specified 'permissible purposes' and requires CRAs to employ procedures to ensure that they provide consumer reports to recipients only for such purposes," according to the testimony. Data brokers who sell "consumer reports" are subject to the FCRA restrictions.

The Gramm-Leach-Bliley Act imposes privacy and security obligations on a broadly defined group of financial institutions, including those engaged in banking, lending, and insurance activities as well as loan brokering, credit reporting, and real estate settlement services. "To the extent that data brokers fall within the definition of financial institutions, they would be subject to the Act," Majoras said.

In addition, the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce. Prohibited practices include deceptive claims that companies make about privacy, including claims about the security they provide for consumer information," the testimony says. "The Commission has brought five cases against companies for deceptive security claims, alleging that the companies made . . . promises to take reasonable steps to protect sensitive consumer information. Because they allegedly failed to take such steps, their claims were deceptive."

"The Commission is committed to ensuring the continued safety of consumers' personal information," Majoras said.

The Commission vote to authorize the testimony was 5-0.

Copies of the testimony are available from the FTC's Web site at http://www.ftc.gov and also from the FTC's Consumer Response Center, Room 130, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint in English or Spanish (bilingual counselors are available to take complaints), or to get free information on any of 150 consumer topics, call toll-free, 1-877-FTC-HELP (1-877-382-4357), or use the complaint form at http://www.ftc.gov . The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Media Contact:

Claudia Bourne Farrell
Office of Public Affairs
202-326-2181

(FTC File No. 052 3069)

E-mail this News Release
If you send this link to someone else, the FTC will not collect any personal information about you or the recipient.

Related Documents:

Prepared Statement of the Federal Trade Commission On Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, Presented by Chairman Deborah Platt Majoras Before the Committee on Banking, Housing, and Urban Affairs of the United States Senate (March 10, 2005).

Consumer Information:

- ID Theft

Last Modified: Monday, 25-Jun-2007 16:20:00 EDT

EXHIBIT D

THE WHITE HOUSE
PRESIDENT
GEORGE W. BUSH

CLICK HERE TO PRINT

For Immediate Release
Office of the Press Secretary
July 15, 2004

President Bush Signs Identity Theft Penalty Enhancement Act

Remarks by the President at Signing of Identity Theft Penalty Enhancement Act
Roosevelt Room

en Español

10:52 A.M. EDT

THE PRESIDENT: Thanks for coming. Welcome to the White House. Thanks for coming. (Laughter.) Welcome to the White House. (Laughter.)

7/15/04
James B. Comey Deputy Attorney General, discussed the Identity Theft Penalty Enhancement Act on Ask the White House.
Click here to read the transcript

VIDEO Multimedia
President's Remarks
view
listen

We're taking an important step today to combat the problem of identity theft, one of the fastest growing financial crimes in our nation. Last year alone, nearly 10 million Americans had their identities stolen by criminals who rob them and the nation's businesses of nearly $50 billion through fraudulent transactions. The bill I'm about to sign sends a clear message that a person who violates another's financial privacy will be punished.

The Identity Theft Penalty Enhancement Act also prescribes prison sentences for those who use identity theft to commit other crimes, including terrorism. It reflects our government's resolve to answer serious offenses with serious penalties.

I appreciate the members of my administration who worked on this important piece of legislation, particularly Cabinet members John Snow and John Ashcroft. I appreciate the members of the Congress who worked hard on this legislation: Senator Orrin Hatch and Senator Jon Kyl, Senator Dianne Feinstein, and members of the House, Chairman, Senator Jim Sensenbrenner, and John Carter from the great state of Texas. I want to thank the other members of Congress who are here, members of both political parties. Thank you for coming. I thank those who are on their staffs who have worked hard.

The crime of identity theft undermines the basic trust on which our economy depends. When a person takes out an insurance policy, or makes an online purchase, or opens a savings account, he or she must have confidence that personal financial information will be protected and treated with care. Identity theft harms not only its direct victims, but also many businesses and customers whose confidence is shaken. Like other forms of stealing, identity theft leaves the victim poor and feeling terribly violated.

But the losses are not measured only in dollars. An identity theft -- thief can steal the victim's financial reputation. Running up bills on credit card accounts that the victim never knew existed, the criminal can quickly damage a person's lifelong efforts to build and maintain a good credit rating. Repairing the damage can take months or years.

Government has a responsibility to protect citizens from these crimes and the grief and hassle they cause. It's a solemn responsibility of our government. I want to thank the members of Congress for recognizing that responsibility.

This good law is part of a broader effort we've waged in recent years. The U.S. Postal Inspection Service, the FBI, and Secret Service are working with local and state officials to crack down on the criminal networks that are responsible for much of the identity theft that occurs in this nation. The Federal Trade Commission is training local law enforcement in the detection of identity theft. The Commission has set up the ID Theft Data Clearinghouse, which keeps track of complaints across the country, and provides those records to prosecutors seeking to take

down organized rings.

Last December, I signed the Fair and Accurate Credit Transactions Act, which established a national system of fraud detection so that identity thieves can be stopped before they run up tens of thousands of dollars in illegal purchases. Thanks to this law, victims can make one phone call to alert all three major credit rating agencies to report the crime and to protect their credit ratings.

The law I sign today will dramatically strengthen the fight against identity theft and fraud. Prosecutors across the country report that sentences for these crimes do not reflect the damage done to the victim. Too often, those convicted have been sentenced to little or no time in prison. This changes today. This new law establishes in the federal criminal court the offense of aggravated identity theft. And someone convicted of that crime can expect to go to jail for stealing a person's good name. These punishments will come on top of any punishment for crimes that proceed from identity theft. For example, when someone is convicted of mail fraud in a case involving stolen personal information, judges will now impose two sentences, one for mail fraud, and one for aggravated identity theft. Those convicted of aggravated identity theft must serve an additional mandatory two-year prison term. Someone convicted of aggravated identity theft, such as using a false passport in connection with a terrorism case, would receive an additional prison sentence of five years. In addition, judges will not be allowed to let those convicted of aggravated identity theft serve their sentence on probation.

This law also raises the standard of conduct for people who have access to personal records through their work at banks, government agencies, insurance companies, and other storehouses of financial data. The law directs the United States Sentencing Commission to make sure those convicted of abusing and stealing from their customers serve a sentence equal to their crimes.

What I'm telling you is this is a good law. And I appreciate you working hard to see to it that it made it to my desk. Because of this act of Congress I sign today, the guilty will be certain to be punished. That's good for our consumers, it's good for our economy, and it's good for the cause of justice.

Welcome to the White House. (Applause.)

(The bill is signed.)

END 10:59 A.M. EDT

Return to this article at:
http://www.whitehouse.gov/news/releases/2004/07/20040715-3.html

CLICK HERE TO PRINT

EXHIBIT E

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JOSEPH A. VIDAL, SR., Plaintiff	:	CIVIL ACTION
v.	:	
EXPERIAN INFORMATION SOLUTIONS, INC., et al., Defendants	:	NO. 04-3867

ORDER

AND NOW, this 3rd day of February, 2005, upon consideration of defendant Experian Information Solutions, Inc.'s ("Experian") motion for protective order (Docket No. 16), plaintiff's opposition thereto, defendant's reply, and after oral argument held on February 1, 2005, IT IS HEREBY ORDERED that said motion is GRANTED. IT IS FURTHER ORDERED that the parties shall comply with the protective order submitted to the Court with the motion.

Experian has requested a protective order to maintain the confidentiality of four categories of documents: the administrative report; the dispute response log; the disclosure request log; and, the transaction log. Experian concedes that they are discoverable but asks the Court to order that they be kept confidential during this litigation, used only for purposes of this litigation, and returned at the end of the litigation.

Under Fed. R. Civ. Pro. 26(c), "for good cause shown," the Court may issue a protective order that a trade secret or other confidential research, development, or commercial information not be revealed or revealed only in a designated way." Experian has filed an affidavit of a Consumer Affairs Specialist in its National Consumer Assistance Center in support of the motion. The affidavit establishes to the Court's satisfaction that certain information in these documents is a trade secret and should remain confidential. These documents were created in response to this lawsuit to investigate the plaintiff's claim. They relate to the plaintiff but contain certain confidential codes that a competitor could use to reverse-engineer the design of Experian's System. The affidavit is fourteen pages in length and with specific detail explains the documents and why they contain proprietary information.

The plaintiff argues that the Court should not grant the motion because documents of the type at issue here were produced in another case without a protective order. In that case, a junior lawyer representing Experian handed over in discovery documents that would fall into two of the categories at issue here. Experian moved for a protective order with respect to documents in the other categories at issue here. The court denied that motion.

The plaintiff argues that because those documents were produced in that case, nothing would be gained by granting the protective order because the codes are already in the public domain. Counsel for Experian argued persuasively that it is not the disclosure of one document that would allow the reverse-engineering but the discovery of many documents of this type. The more documents that become publicly available, the easier it would be to reverse-engineer Experian's System. This fact is also reflected in the affidavit. See ¶¶ 48,49.

The plaintiff's main objection to the protective order appears to be that in some cases, it would present a large burden to plaintiff's counsel. Counsel for the plaintiff complained that in some cases, documents are not produced for a month or more while the parties try to negotiate a protective order. He complained that having such an order would be difficult if the plaintiff were pro se.

The Court can appreciate the concerns raised by the plaintiff's counsel but the Court cannot make a decision in this case based on the conduct of defense counsel in other cases. In this case, Experian has already produced a large number of documents without any claim of confidentiality. It is only those documents that fit within these four categories that they have withheld. Whether or not a protective order should be issued in any given case depends on the circumstances of that case. If,

indeed, more of these documents become part of the public domain, it may be that Experian is not competitively disadvantaged by the disclosure of a few more. But in this case, the Court is convinced that there would be a competitive disadvantage to Experian if these documents were in the public domain.

The Court is also persuaded that Experian has diligently maintained the confidentiality of the documents. The main argument made by the plaintiff on this issue is that an affiliate of Experian, CBA, had given documents of this type in discovery. Experian presented to the Court the agreement under which CBA should have been protecting those documents and assured the Court that it is taking action to determine whether or not CBA has been producing such documents.

A final concern voiced by the plaintiff was that counsel did not want to be in the position of being charged with violating the protective order if he or someone on his staff inadvertently fails to file a confidential document under seal. But there is nothing in the proposed protective order that would allow such a claim for an inadvertent disclosure. The Court has handled many cases with a protective order in place. If someone by mistake fails to file a confidential document under seal, the document is placed under seal once the party realizes the mistake. There would be no penalty for such an inadvertent disclosure.

BY THE COURT:

/s/ Mary A. McLaughlin

MARY A. McLAUGHLIN, J.

CERTIFICATE OF SERVICE

I hereby certify that on this 3rd day of December 2007, a copy of the foregoing was served via ECF and U.S. mail, postage prepaid, upon the following:

Mark D. Mailman, Esq.
FRANCIS & MAILMAN, P.C.
Land Title Building, 19th Floor
100 South Broad Street
Philadelphia, PA 19110

/s/ Mohammad A. Ghiasuddin
Counsel for Defendant
EXPERIAN INFORMATION SOLUTIONS, INC.